**A Cyber Security White Paper**

# Securing Process Control Network External Communications



Honeywell

# Securing Process Control Network
# External Communications

## Introduction

In an ideal Process Control Network (PCN) security scenario, the PCN would not need to communicate with any external systems. Not only could an air-gap be created, providing excellent security, there would also be no costs for connectivity and security solutions. In the real world, however, sharing PCN data with external systems and accessing PCN systems from external sources is fast becoming a business necessity. This paper provides some generic guidelines for enabling secure connectivity between PCNs and external systems. Please note that there are enumerable security measures that one can apply to these communications, however, security is always a balance of:

- The value of assets being protected
- The cost of the security measures protecting the assets, and
- The inconvenience imposed by the security measures

This paper outlines one possible solution for balancing these factors.

The drawing in "Figure A" depicts a generic and simplified representation of an interface between a PCN and Enterprise Network and will be referred to often, so the reader can better visualize the scenarios, issues and proposed solutions to each. It is therefore appropriate to discuss this generic drawing in a little more detail. The drawing contains a firewall with three interfaces. One interface connects to the PCN, one to the Enterprise network and one to a DMZ network.

## Definitions

Definition of the networks mentioned above:

- The **PCN (Process Control Network)** is the protected asset. Considered a real-time mission critical asset, it is key to the success of the corporation. It may also contain data and information that is extremely valuable in making business decisions. The details, of what the PCN contains, vary widely from industry-to-industry and even company-to-company. Therefore, for the purpose of this paper, the PCN systems accessed and protected are process control systems, Ethernet connected, running on Open Operating Systems and communicating via the TCP/IP protocol.
- Consider the **Enterprise Network** as anything outside of the Process Control Network. This includes the local site network, corporate WAN network and possibly Engineers working at home or from hotels through the Internet. Although this paper considers the Enterprise Network the unsafe entity, from which the PCN is protected, implementation of security measures contained in this paper will also help to protect the Enterprise Network from the PCN.
- The **DMZ or Demilitarized Zone** is a critical piece of the PCN security puzzle since it can be used as a buffer/proxy zone for communication between the PCN and the Enterprise Network. The servers/systems on the DMZ should be hardened and continually updated with the latest security patches and anti-virus files. Communications to and from these systems need to be restricted by the firewall to the greatest extent possible. Exactly what the servers, on this segment, are for will become clear in the scenarios and issues that follow.

**Ideally, in the environment just outlined, there will be no direct communication between the Enterprise Network and the PCN**. All communication will take place through the hardened DMZ servers. This may not always be possible but should be the goal.

The first PCN connectivity issue that companies usually experience is the need for Data, Information and/or graphs from the PCN to help people and/or systems on the Enterprise Network make business decisions.

Usually a Data Historian Server and/or Data WEB server provides this information. "Figure A" contains the generic term **Data Server**. These servers collect data from on-process control systems and make the information available to users on the enterprise network. There is nothing new about these Data servers, so why put them on a DMZ? Communication to a Data Server should be restricted as much as possible. This is true whether the data server is collected/receiving data from a PCN system or providing data to an end user/system on the Enterprise network. Locating the Data Server on the DMZ allows the application of full firewall controls on all communications to and from the Data Server whether the communication is with the Enterprise network or the PCN.

Another connectivity issue is how to allow Engineers that are not physically on the PCN, to access the systems on the PCN. Engineers may need access for a number of reasons including tuning, trouble-shooting, maintenance or Screen design. There are definite issues with an Engineer accessing PCN systems directly from an Enterprise System.

One issue is that a PCN system may not be running the latest OS security patches or latest anti-virus files. This is not necessarily because the site has not gotten around to patching the systems yet, but could very well be that the patches and/or anti-virus files have not yet been tested, certified and blessed by the Process Controls Vendor. This makes PCN systems vulnerable to worms and viruses. It is therefore necessary to make sure that the remote engineer's PC is hardened, patched and has an up-to-date anti-virus. Unfortunately, keeping track of and controlling all of the Engineers' desktops, laptops and home systems is not always possible. This is where utilization of the **Terminal Server** on the DMZ comes into play. If all remote Engineering access to the system on the PCN comes through a Terminal Server on the DMZ, then the only system directly communicating with PCN systems is this one terminal server. It is now very easy to make sure that this one system is hardened, patched and equipped with the latest anti-virus.

Utilizing a Terminal Server for remote Engineer PCN access also addresses another issue. That is **authentication**, **authorization** and **accounting**. The terminal server will make the engineer **authenticate** who he or she is by providing a username and password. More security can be provided by requiring two-factor authentication, but that will not be discussed here. This is much more secure than just allowing an IP address through a firewall, since it allows access based on who someone is rather than what IP address they have. Once logged into the terminal server, the terminal server can control the exact system(s) on the PCN to which the Engineer has **authorization** to connect. In addition, the Terminal Server can keep an **accounting** record of which engineers were connected to which PCN systems and at what time.

Another potential issue is updating patches and anti-viruses on the PCN. If it is done directly from the Enterprise Network, that is contrary to the goal of not having direct communication between the PCN and Enterprise Network. Honeywell therefore recommends that a **Patch Manager Server** and an **Anti-Virus Server** be located directly on the DMZ. It is very possible that these two functions reside on a single server. Having Patch Management and Anti-virus Management dedicated to the PCN allows for controlled and secure updates that the user can tailor for the unique needs of the Process controls environment. It also helps address the issues that arise when the anti-virus product that is supported by the process controls vendor is not the same as the anti-virus product supported by the corporate IT department.

The aforementioned security measures should not be viewed in a vacuum. There are many other considerations such as Intrusion Detection, security policy, physical security, security education, security incident response, contingency, disaster recovery and many more. The intent of this paper was to help identify certain needs and issues unique to the Process Control Environment as well as provide some ideas for solutions.

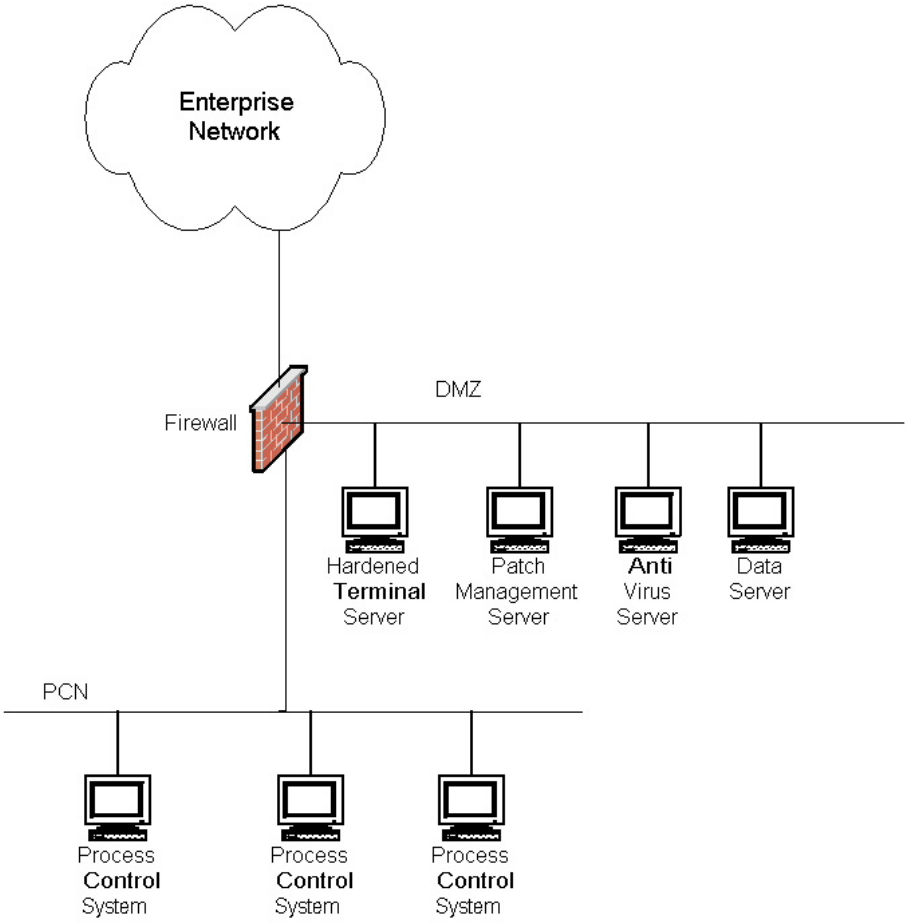


**Figure A – Generic and Simplified Representation of an Interface between a PCN and an Enterprise Network**